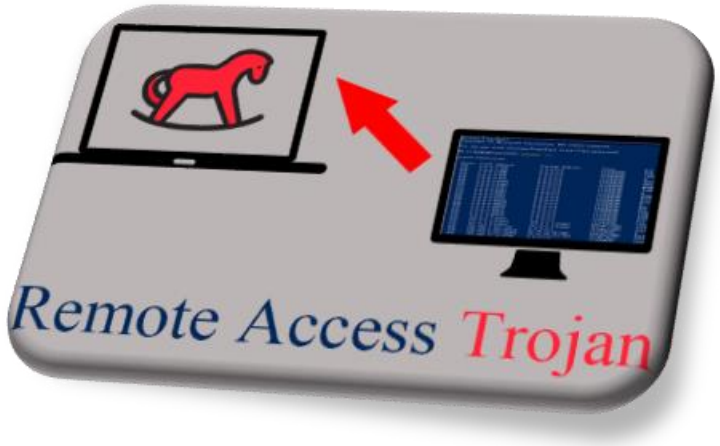
WINDOWS RED TEAM OPERATOR

Malware Analysis & Development w/t Practical & Hands-On



Windows Malwares (RATs & Trojans)

Malware Types & Classification:

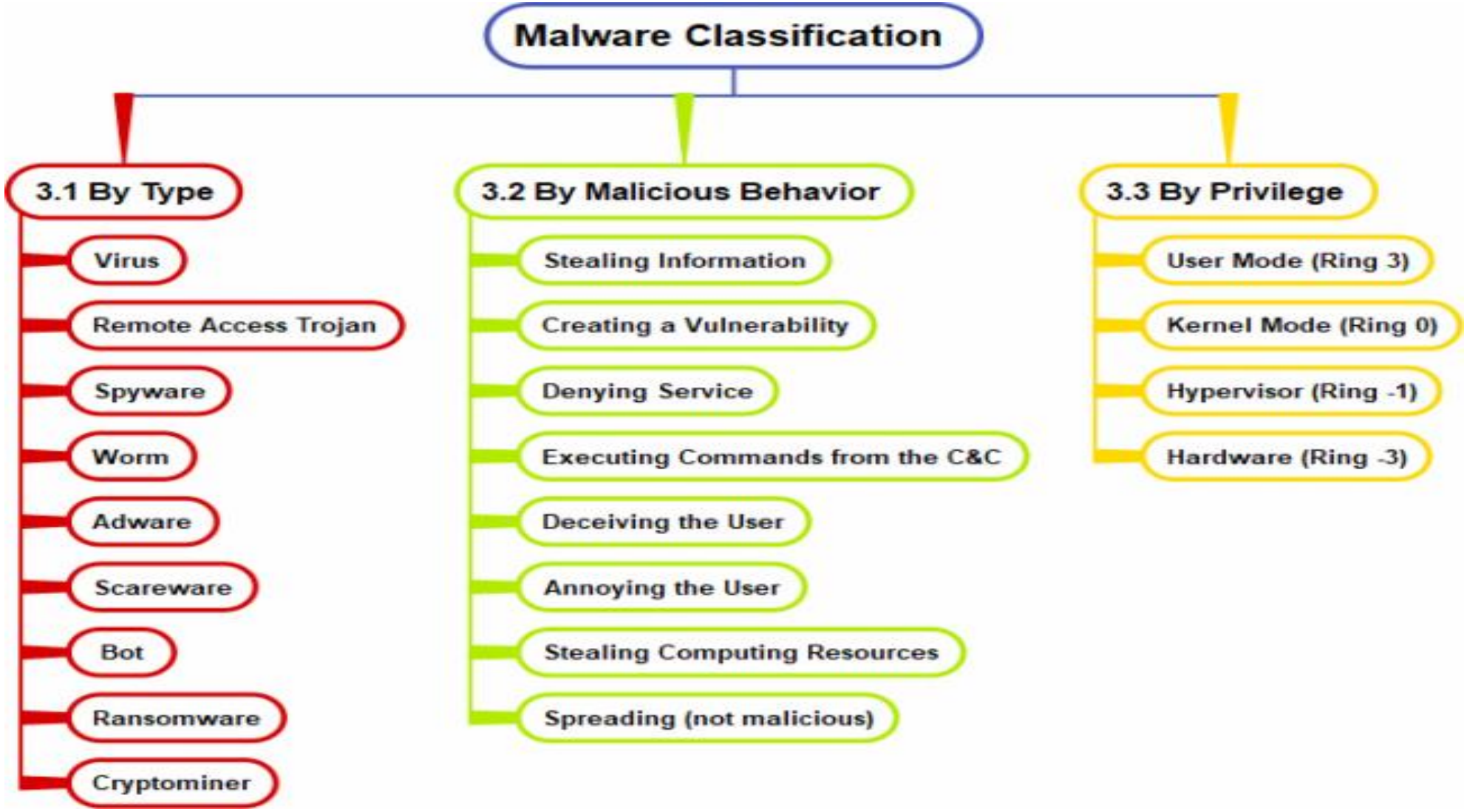


Fig. 1. Various malware taxonomies. (*)

Malware Behavior:

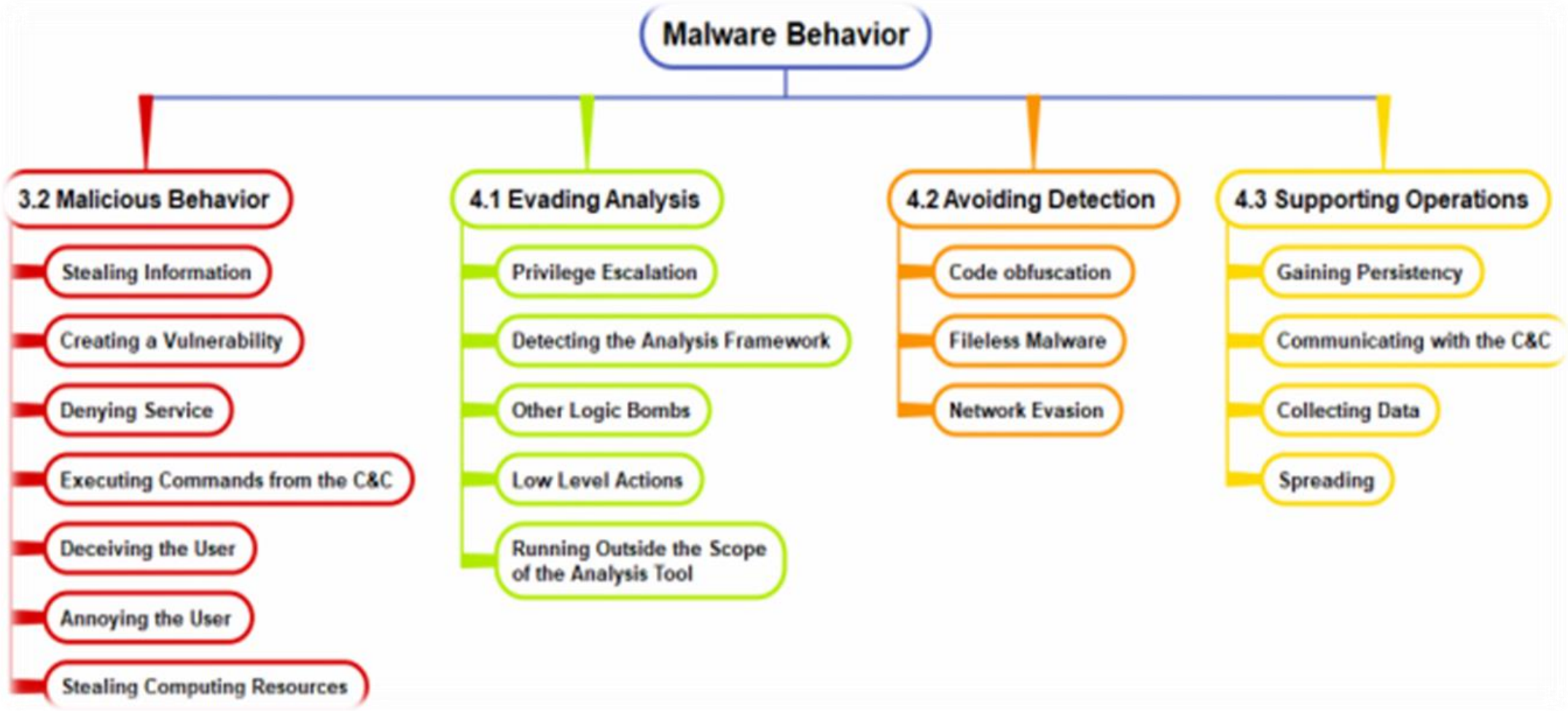
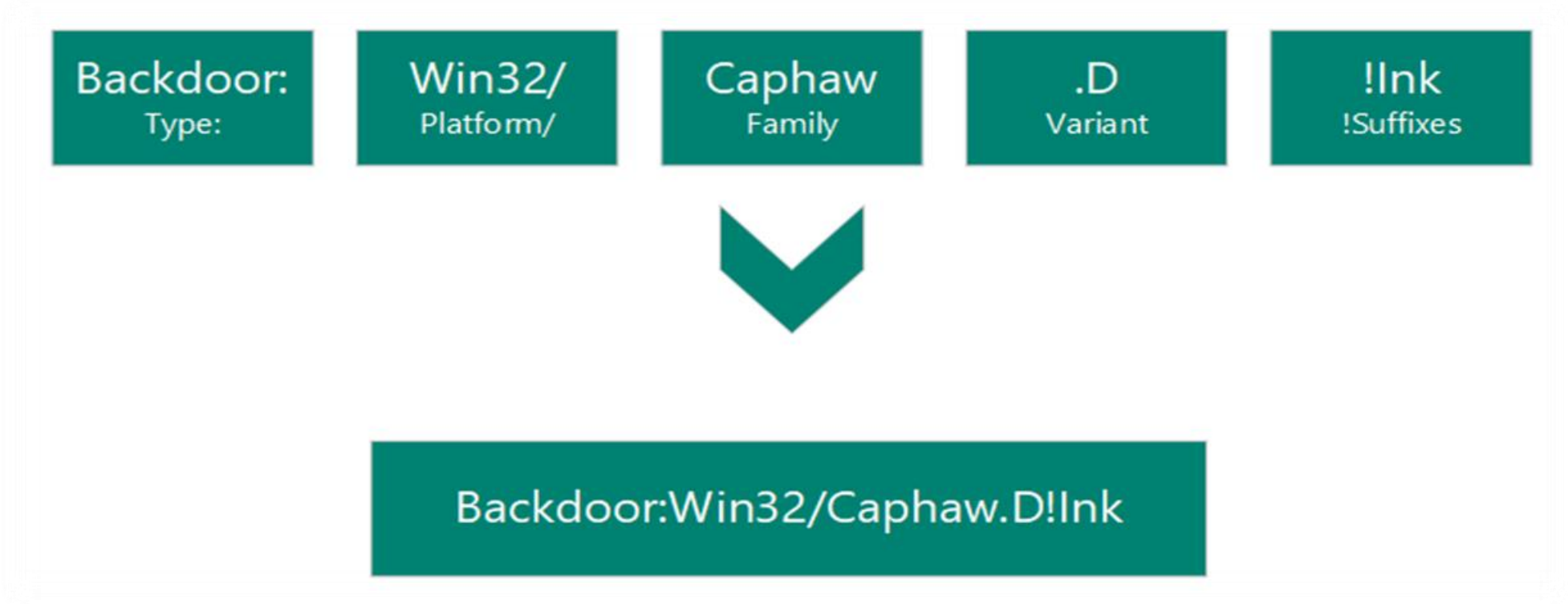


Fig. 2. Malware Behavior Taxonomy (*)

Windows Malware Naming:

Microsoft names the malware and unwanted software that is detect according to the Computer Antivirus Research Organization (CARO) malware naming scheme.

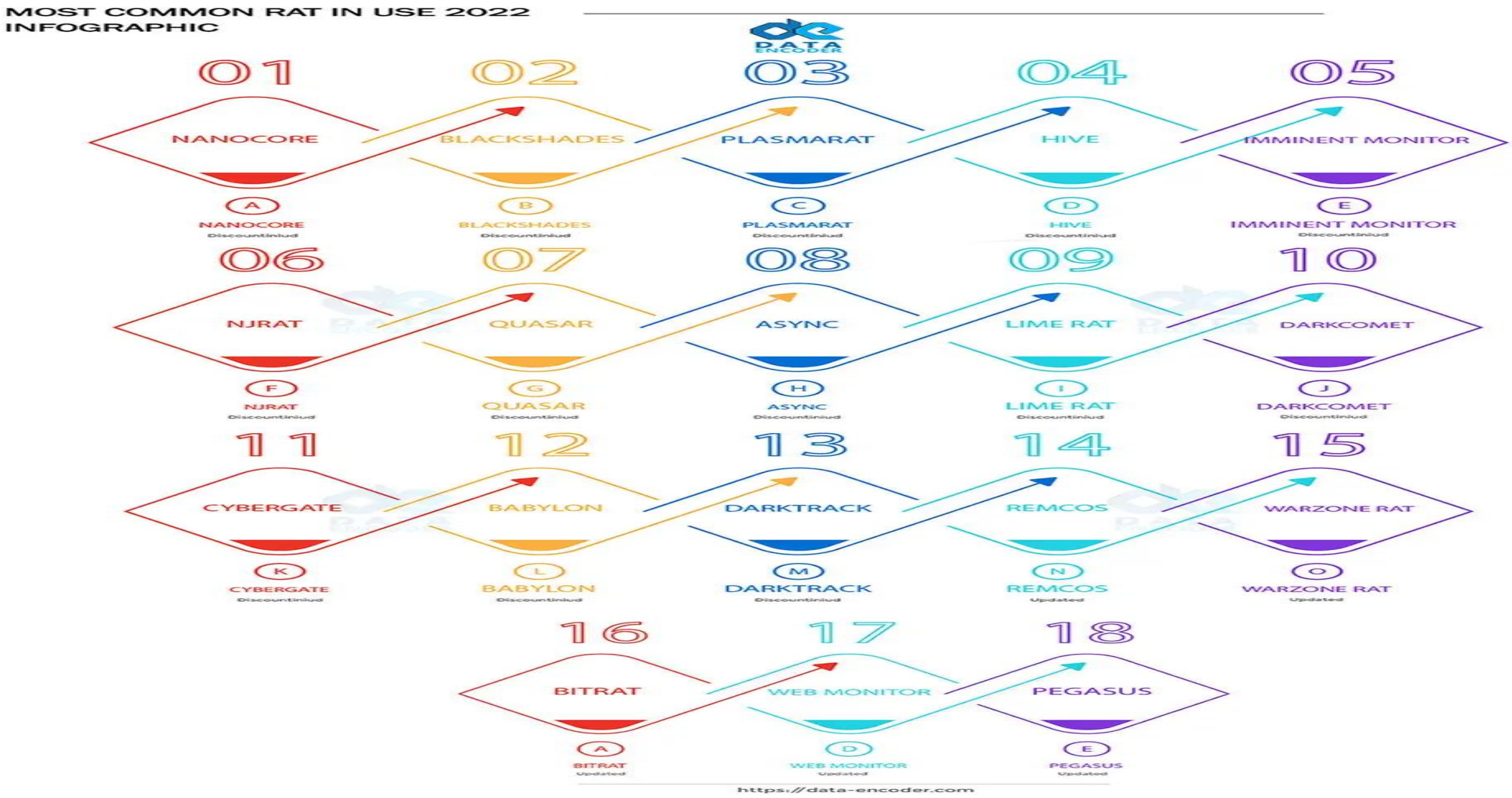
The scheme uses the following format: (Link)



Windows Malware & Other Threats:

- Coin miners
- Exploits and exploit kits
- Macro malware
- Phishing
- Ransomware
- Rootkits
- Supply chain attacks
- Tech support scams
- Trojans
- Unwanted software
- Worms

Common Windows Remote Access Trojan:



Windows Remote Access Trojan:

- Quasar (https://github.com/quasar/Quasar)
- Dc RAT (https://github.com/qwqdanchun/DcRat)
- Lime-RAT (https://github.com/NYAN-x-CAT/Lime-RAT)
- AsyncRAT (https://github.com/NYAN-x-CAT/AsyncRAT-C-Sharp)
- VanillaRAT (https://github.com/DannyTheSloth/VanillaRAT)
- EagleMonitor (https://github.com/arsium/EagleMonitorRAT)

WINDOWS MALWARES (RATS & Trojans)

Practical & Hands-On Demo of various Windows OPEN-SOURCE RATs

- Installation ..
- Working & Usages ..
- Additional Tips & Notes..
- Safety Measures & Precautions..